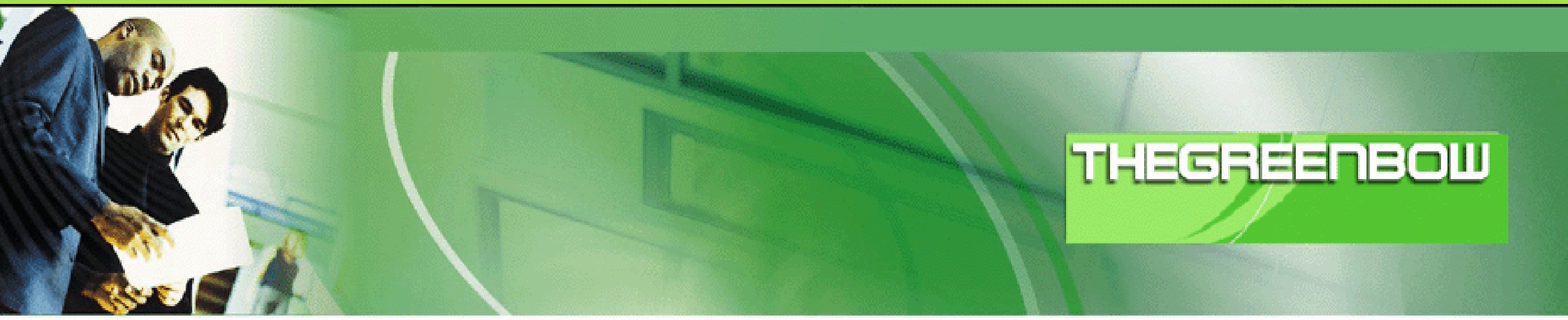


TheGreenBow CryptoMailer

User Guide

Contact: support@thegreenbow.com

Website: www.thegreenbow.com

CryptoMailer User Guide

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: février 2009 in San Francisco.

Table of Contents

Part I

Introduction

1 Introduction

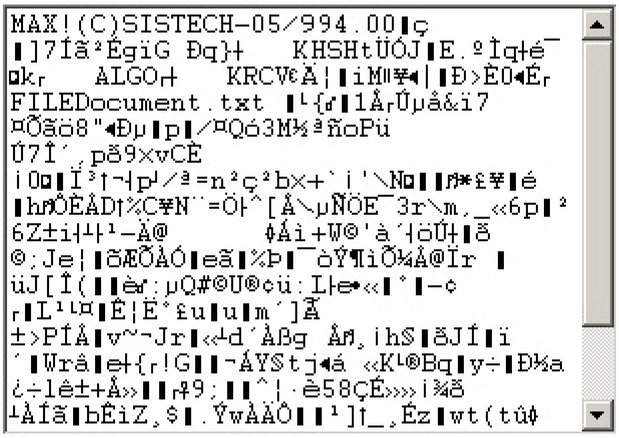
1.1 Why and how to encrypt

Why encrypting emails

The emails you send today are transmitted over the Internet machine to machine without any protection or privacy: exactly like postcards.

Thus, your colleagues, your email administrator, your access provider, equipment which provide for the transit of data over the Internet, the provider of your correspondent, his email administrator, his staff, all those equipments or people may read your emails.

Using CryptoMailer, your messages will be encrypted.
So your messages can be intercepted ... but they are unreadable, except for your recipient who holds the secret to decipher them.



```
MAX!(C)SISTECH-05/994.00▮ç
▮]7Îã²ÉgïG Ðq}┼   KHSHtÜÓJ▮E.ºÌq┼é¯
◘kr   ALGO┤   KRCV€Ä¦▮iM‼¥◄|▮Ð>ÈO◄Ér
FILEDocument.txt ▮└{♂▮1ÅrŮµå&ï7
¤Õãö8"◄Ðµ▮p▮/¤Qó3M¾ªñoPü
Ú7Î´¸pð9xvCÈ
¡O◘▮Ï³↑¬┤p┘/ª=n²ç²bx+`¡'\№▮▮ŋ*£¥▮é
▮hŋÔÈÅD↑%C¥N¨=Ö├^[Å\µÑÖE¯3r\m,_«6p▮²
6Z±i┤┴├¹-Ä@      ¢Ái+W©'à´┤öÚ┼▮ð
©;Je¦▮õÆÕÀÓ▮eã▮%Þ▮¯òÝ¶iÕ¾Å@Ïr ▮
üJ[Î(▮▮è♂:µQ#©U®¢ü:L├e•«▮˚▮-¢
r▮L¹└¤▮Ê¦Ë˚£u▮u▮m´]Ã
±>PÍÅ▮v~¬Jr▮«┴d´ÀBg Åŋ¸¡hS▮ðJÍ▮ï
´▮Wrâ▮e┼{r!G▮▮¬ÁYStj◄á «K└®Bq▮y÷▮Ð¾a
¿÷lê±+Å»▮▮r┼9;▮▮^¦·è58ÇÉ»»¡¾ð
┴ÀÍã▮bÊiZ¸$▮.ŸwÀÄÔ▮▮¹]↑_¸Éz▮wt(tû¢
```

How to encrypt

Whenever a file is encrypted by CryptoMailer, a random key is created. This key is protected by a protection key derived from a user password. This password can be chosen from the list or entered manually.

This way, the same document encrypted several times with the same password gives different results. It is therefore impossible to decrypt a document for someone who does not know the password.

Brute force

To find the password, a method of "brute force" can be used. This method consists of trying all possible strings. So depending on complexity of the password, the brute force method is quickly becoming useless, due to the extremely high number of combinations to test.

Assuming the password "k5L;@y=P". To find this password composed of eight characters, an attacker must try all possible codes between 1 and 8 characters, to have the chance to find it.

Consider that there are 112 characters "easily" accessible by a computer keyboard: the tiny, capital letters, numbers, accented characters, punctuation and other symbols. There is no less than 2.5 x 10e +16 codes of eight characters (25 million billion). Assuming that the pirate has a system of computers that allows him to test and verify a million codes per second, it will have nearly 800 years to test all possible codes.

Dictionary
For obvious reasons, there are few people who choose a password like "k5L;@y=P". The hackers thus prefer another method called "Dictionary" attacks.

In a dictionary attack, hackers do not test a sequence of random characters, but likely channels: all words of the English language, names, names, and their combination with some figures e.g."Virginia" and "Jerusalem" will be systematically tested, and probably "virginie35" too.

Such dictionaries exist in all languages, and are fairly easy to find on the internet. Therefore, assuming that the dictionary includes 50000 words, it would need a sentence of at least 3 words to obtain a satisfactory level of security.

Indeed, there are 2.5 billion possible combinations of two words among 50000. With a computer system capable of achieving 1 million operations per second, it will take less than 42 minutes to test them all.

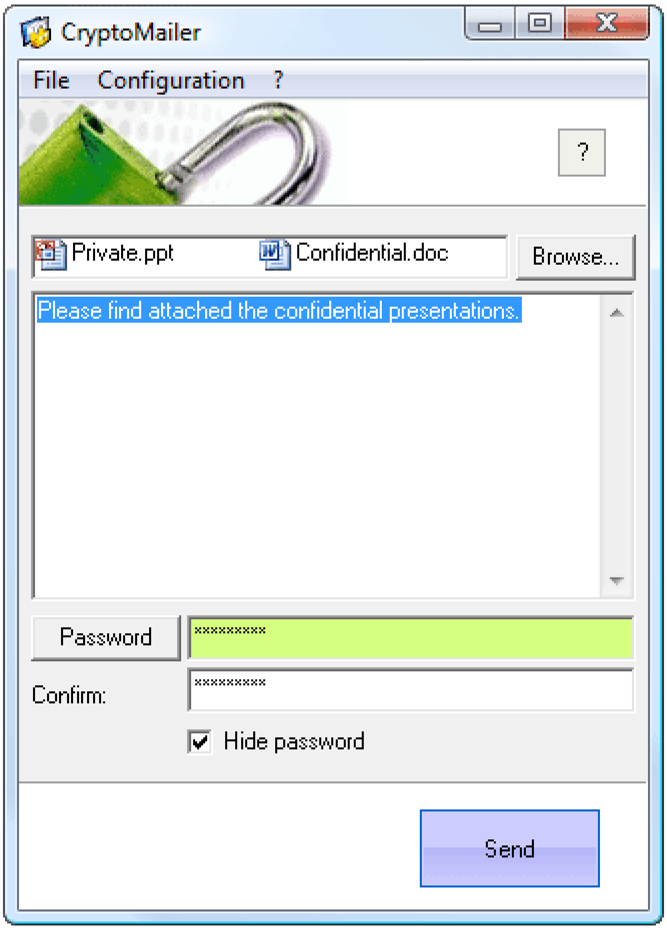
Anyway, even if the string is longer, "strongly holidays" protects much less that "k5L;@y=P". But without doubt, "strongly holidays" provides an adequate level of protection for day to day operations.

Recommendations: It is recommended that meet certain safety rules concerning the composition of passwords.

1.2 Features

CryptoMailer is a tool for encryption of files and messages designed around simplicity of use: Less than a minute after installation, you send your first encrypted email .

CryptoMailer is accessible to encrypt via drag & drop of a file, by the contextual menu of Windows Explorer, or by automatic opening from any messaging software. CryptoMailer encrypts a 3DES or AES 128bit lists of files, with short text message.



Private.ppt Confidential.doc

Please find attached the confidential presentations.

Password: **********

Confirm: **********

CryptoMailer is designed to work with any messaging software (e.g. Outlook, Lotus Notes, Netscape Messenger, Eudora, Pegasus, etc...).

Summary

- Attach short text message
- Work with any messaging software
- Integration into Windows (drag&drop, context menu)
- Contact and password management
- Encryption 3DES, AES 128-bit
- Compression
- Automatic identification password used
- Multi-file encryption
- Import / export of passwords
- Access Control

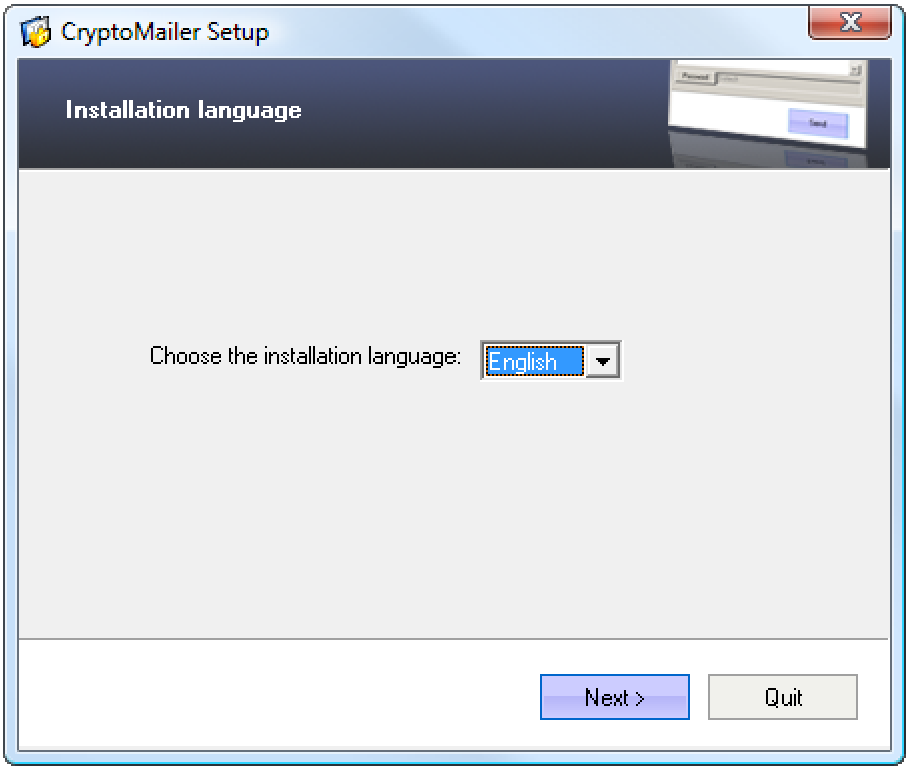
Part II

Getting Started

2 Getting Started

2.1 Installation

The installation of CryptoMailer done in launching the installation software.

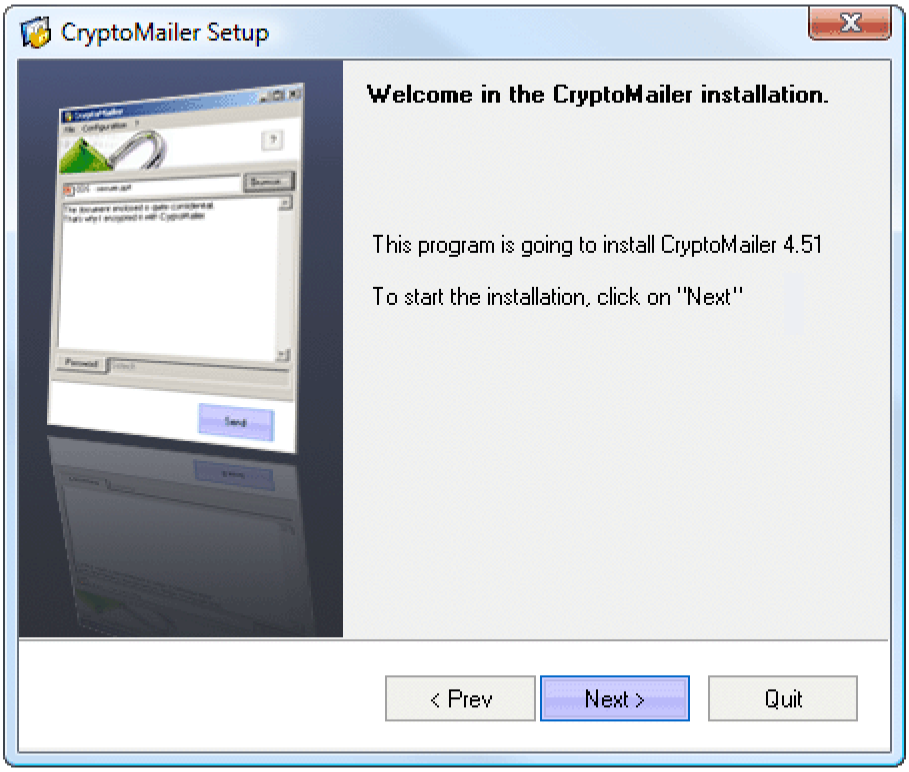


CryptoMailer Setup

Installation language

Choose the installation language: English

The installation of CryptoMailer takes into account a previous version already installed. The configuration of the previous software release (passwords, license number, etc. ...) is automatically preserved by installing the new release.



CryptoMailer Setup

Welcome in the CryptoMailer installation.

This program is going to install CryptoMailer 4.51

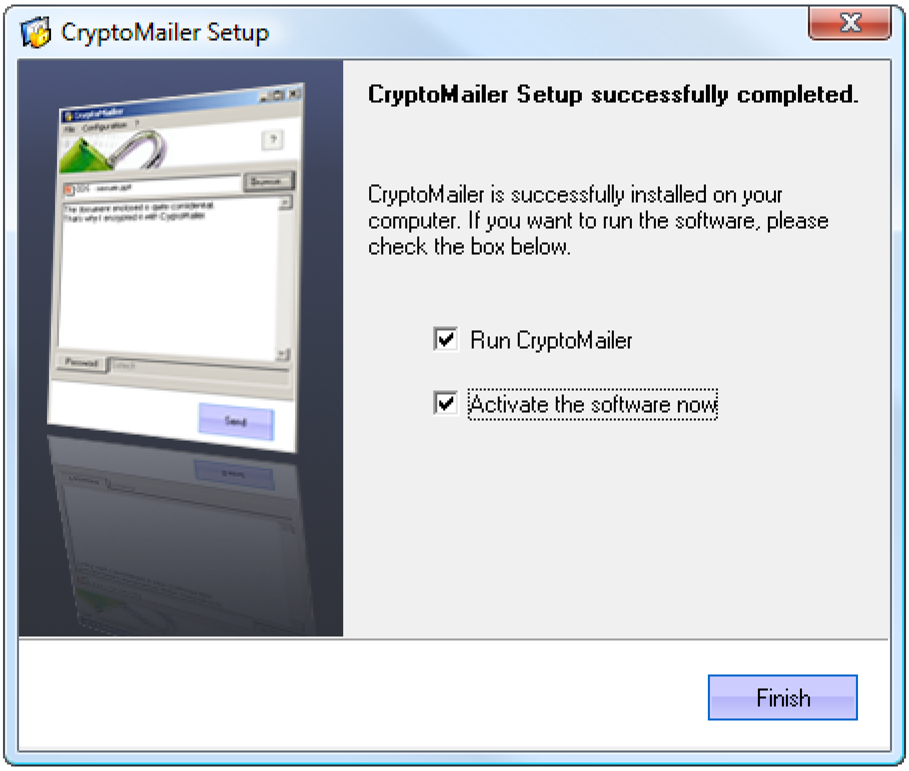
To start the installation, click on "Next"

Important: The installation automatically generates a secret (bi-key).

The secret is stored encrypted **in the CryptoMailer installation directory** in the file "prv".
However, it is recommended to save this secret on another medium disk drive (USB key, etc. ...).

For any recovery of files, the secret is mandatory before contacting our techsupport.

The installation ends with the option to launch and activate the software.



CryptoMailer Setup

CryptoMailer Setup successfully completed.

CryptoMailer is successfully installed on your computer. If you want to run the software, please check the box below.

☑ Run CryptoMailer

☑ Activate the software now

2.2 Installation Problems

During installation, the CryptoMailer files and directories are created. It may happen that some files could not be created if they already exist. If so, the user will be displayed a warning popup window with the file name. Finish the installation, delete that file and start the software installation over again.

Part III

Activation

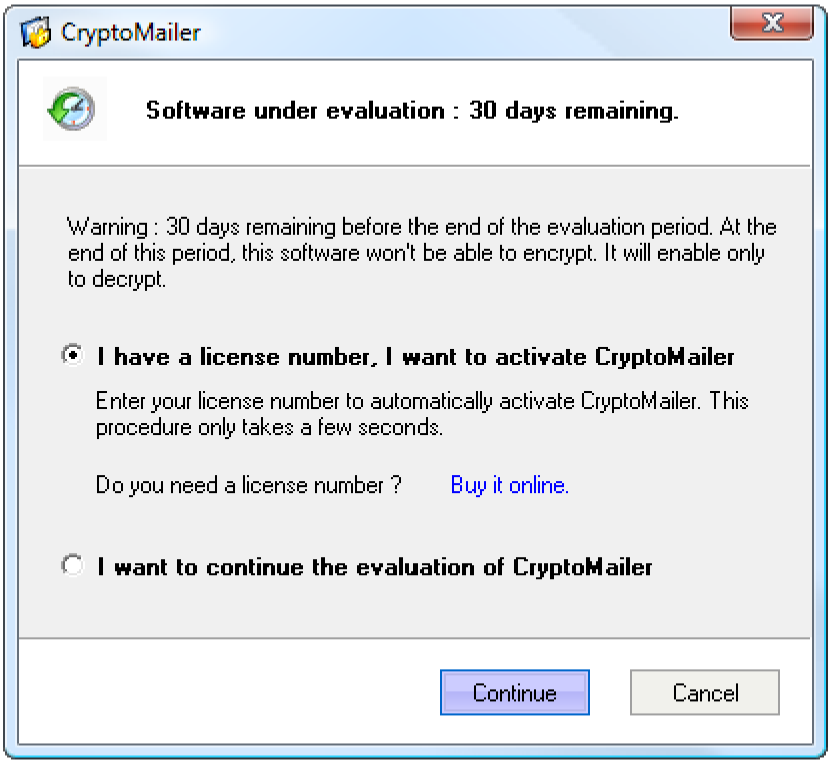
3 Activation

3.1 Evaluation period

CryptoMailer software should be activated before the end of his evaluation period (30 days).

Without activation, the software CryptoMailer continues to operate beyond its evaluation period, but can not encrypt anymore. It can only decrypt.

During the evaluation period, the following window pops up for each encryption:



CryptoMailer

Software under evaluation : 30 days remaining.

Warning : 30 days remaining before the end of the evaluation period. At the end of this period, this software won't be able to encrypt. It will enable only to decrypt.

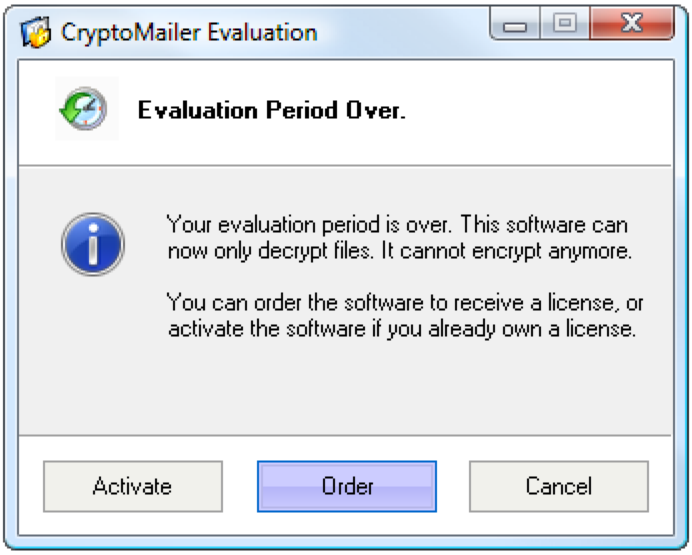
● **I have a license number, I want to activate CryptoMailer**

Enter your license number to automatically activate CryptoMailer. This procedure only takes a few seconds.

Do you need a license number ? Buy it online.

○ **I want to continue the evaluation of CryptoMailer**

Once the evaluation period has expired, the following message appears when the user wants to perform encryption:



CryptoMailer Evaluation

Evaluation Period Over.

Your evaluation period is over. This software can now only decrypt files. It cannot encrypt anymore.

You can order the software to receive a license, or activate the software if you already own a license.

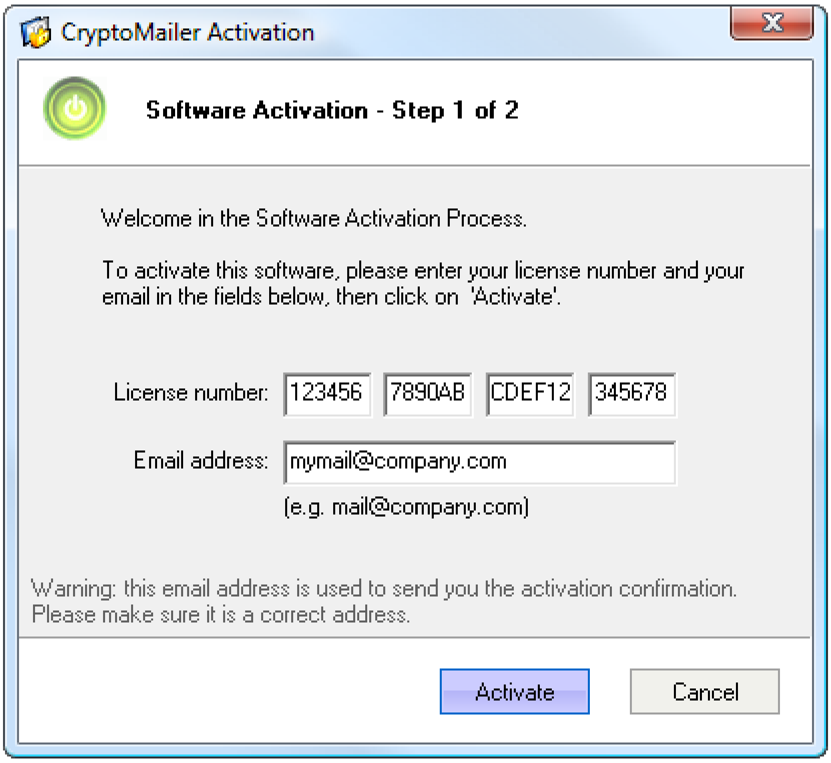
"Order" to purchase a software license online. Once purchased, the software license is automatically and immediately sent by email. See activation.

3.2 Software Activation

CryptoMailer software can be activated at any time, including after the evaluation period, from the menu of the main interface '?' > 'Software Activation'.

Software Activation requires a license number and an email address used to send an activation confirmation.

Simply copy the license number, then click on one of 4 input fields, and paste (Ctrl+V) the license number.



CryptoMailer Activation

Software Activation - Step 1 of 2

Welcome in the Software Activation Process.

To activate this software, please enter your license number and your email in the fields below, then click on 'Activate'.

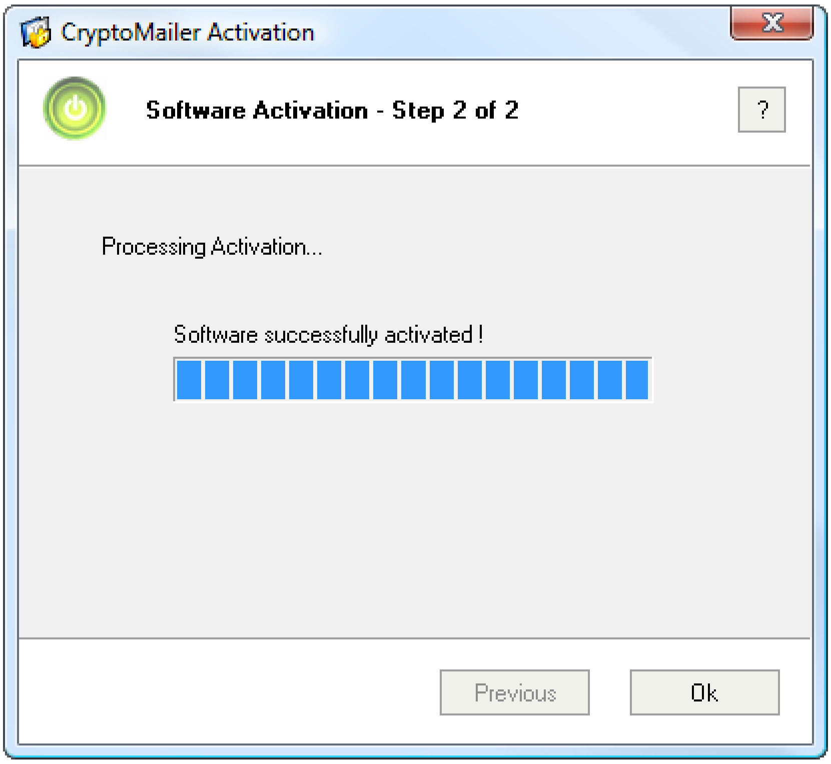
License number: 123456 7890AB CDEF12 345678

Email address: mymail@company.com

(e.g. mail@company.com)

Warning: this email address is used to send you the activation confirmation. Please make sure it is a correct address.

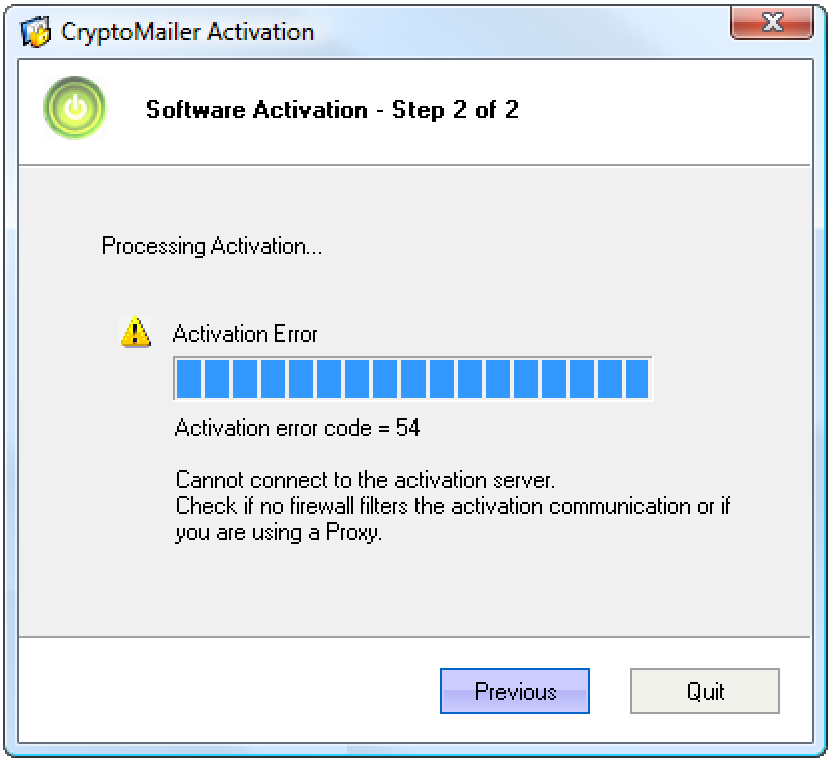
The activation is an exchange with TheGreenBow Online Activation Server. When this exchange succeeds, the activation is complete:



Processing Activation...

Software successfully activated !

The activation may fail for various reasons identified by a code and a narrative:



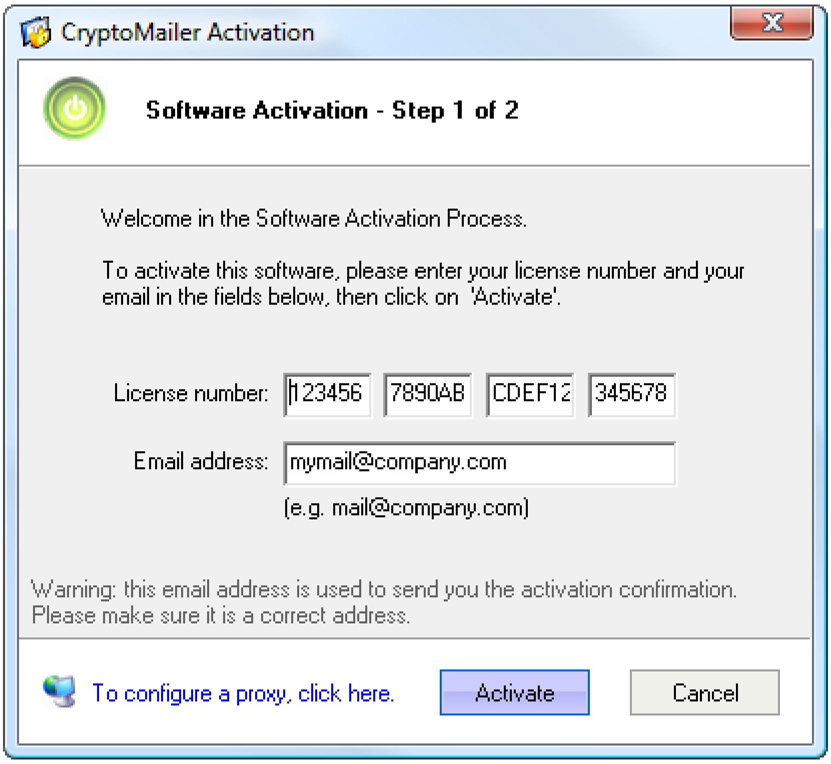
Processing Activation...

Activation Error

Activation error code = 54

Cannot connect to the activation server.
Check if no firewall filters the activation communication or if you are using a Proxy.

In case of network connection problem during activation (error 53 or 54), you can return to previous page to configure a proxy:



CryptoMailer Activation

Software Activation - Step 1 of 2

Welcome in the Software Activation Process.

To activate this software, please enter your license number and your email in the fields below, then click on 'Activate'.

License number: 123456 7890AB CDEF12 345678

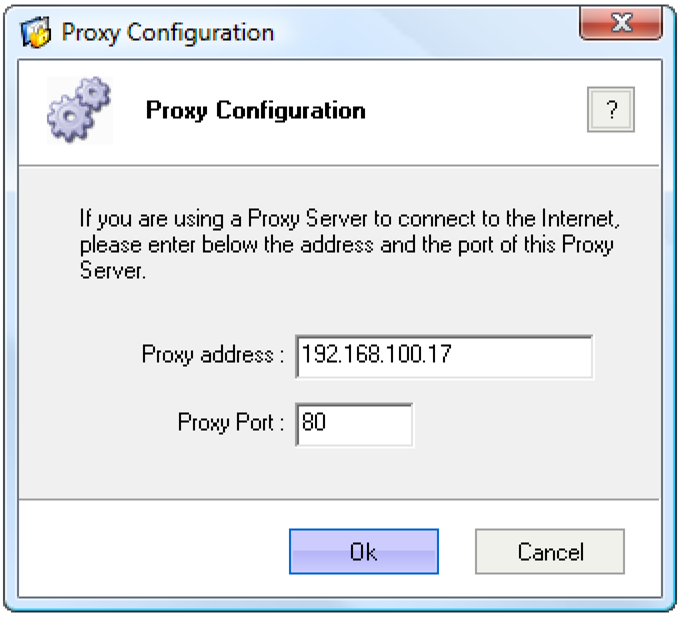
Email address: mymail@company.com

(e.g. mail@company.com)

Warning: this email address is used to send you the activation confirmation. Please make sure it is a correct address.

To configure the proxy, enter the proxy address and port access in the window below.

The address of the proxy may be either an IP address or DNS. The port is a number between 0 and 65535. Typically, the value of the port 80 (HTTP port).



Proxy Configuration

Proxy Configuration

If you are using a Proxy Server to connect to the Internet, please enter below the address and the port of this Proxy Server.

Proxy address : 192.168.100.17

Proxy Port : 80

Part IV

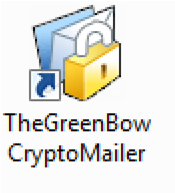
Using CryptoMailer

4 Using CryptoMailer

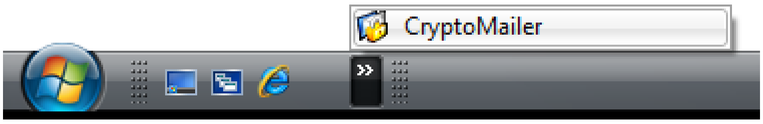
4.1 Launching

CryptoMailer software can be launched in several ways:

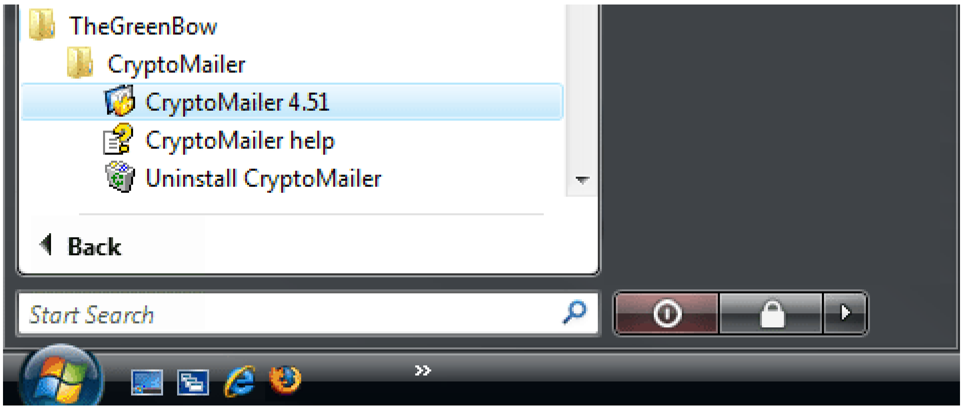
1) from the desktop by double-clicking on its icon.



2) from "quick launch" on the taskbar

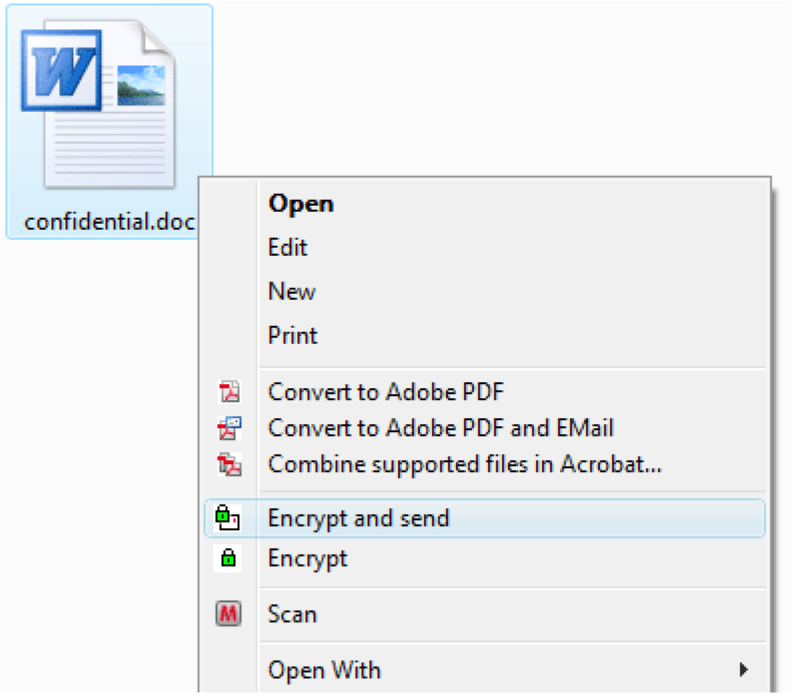


3) from Windows 'Start' menu > 'Programs' > 'TheGreenBow' > 'CryptoMailer'



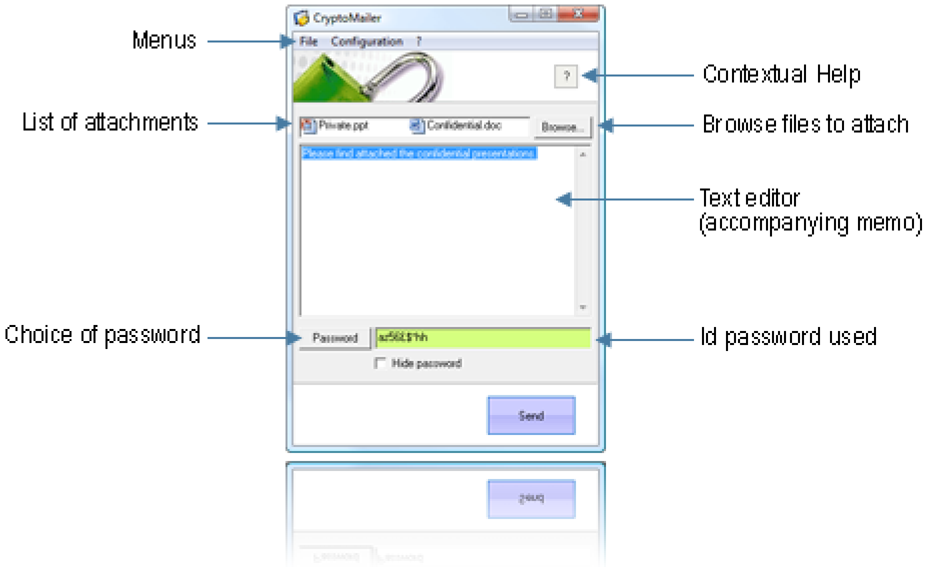
4) via double click on any encrypted file (with ".max" extension)

5) via right-click on a file and selecting "Encrypt and Send" or "Encrypt" (i.e. contextual menu)



4.2 Navigating CryptoMailer

Once started, CryptoMailer presents several areas:



Please find attached the confidential presentations

az582.$*hh

See also:

- Menus
- List of attachments
- Adding a text message
- Choice of password
- Action button like 'Send'

4.3 Menus

1. "File" Menu

The "File" menu is a contextual menu:

- During decryption of email, the "File" menu proposes to "Decrypt as ..." into a directory.
- In the email encryption, the "File" menu proposes "Encrypt as ..." into a directory. The "File" > "New" menu can also empty the text and the file areas.

2. "Configuration" Menu

The "Configuration" menu allows the following features:

- Access to "Password list"
- Protection CryptoMailer software with "Access Control"
- CryptoMailer "Options"settigns

3. "?" Menu

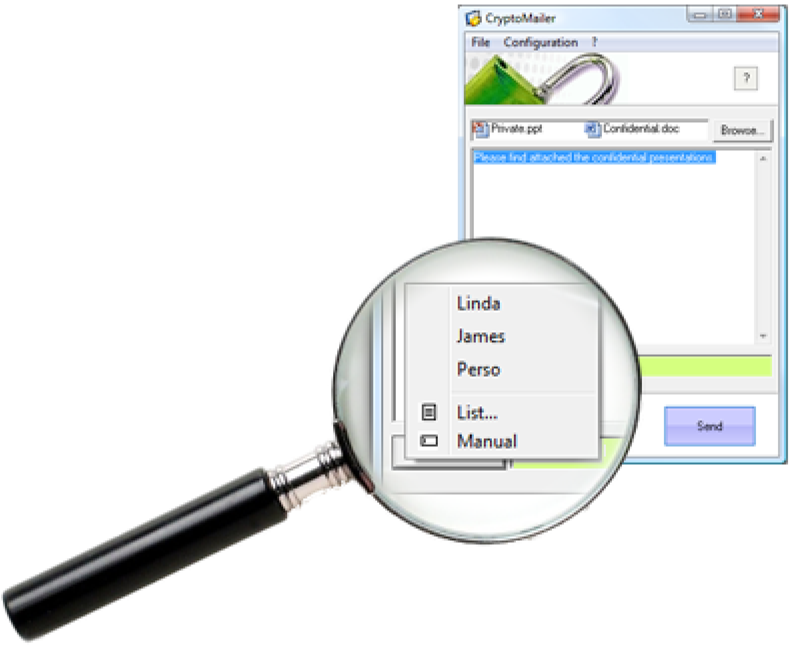
The "?" menu allows the following features:

- Access to "Help"
- Access to online support
- Online Software Activation (this menu disappears once activated)
- "About" windows

4.4 Password choice

CryptoMailer has an intuitive management of passwords.

The choice of a password is immediately accessible from the "Password" button on the main interface. To use a password, simply select from the list:



Please find attached the confidential presentations

The drop-down menu associated with the "Password" button offers at any moment:

- A list of already defined passwords,

- To acccess to the management of passwords ("List ...") to add, change or delete a password,
- To enter a password manually without picking it from the password list ("Manual").

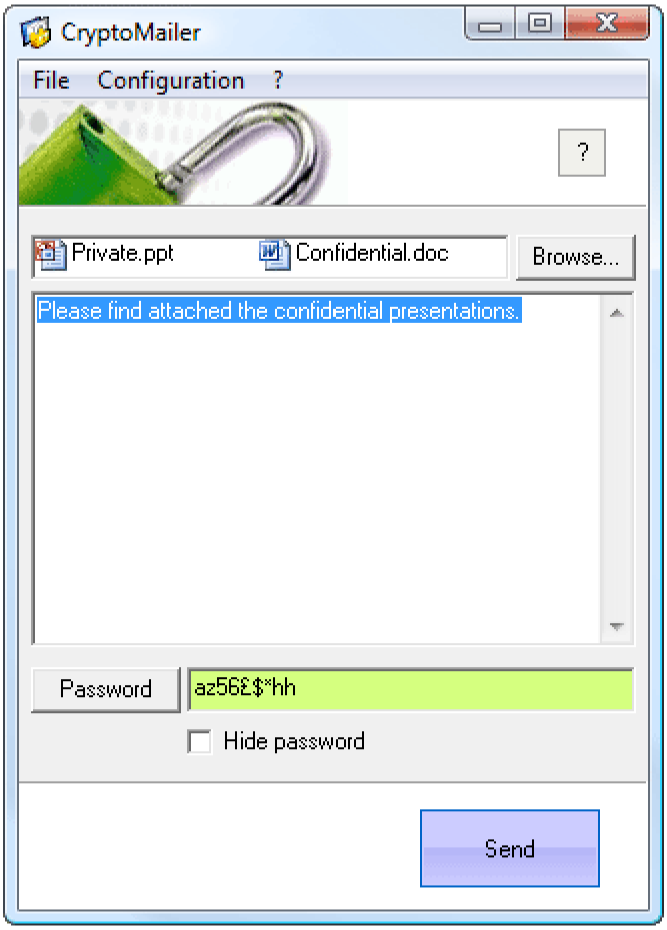
1. Choosing a password in the list
CryptoMailer will store an unlimited number of passwords. Once stored (see Management passwords), they are not readable. You can associate the name of email recipient you are going to send email to.

Saving passwords and recipient names allows the software to find automatically the right password for each decryption when decryption is requested.

2. Entering password manually (menu "Manual")
When the mode "Manual" is selected, the box on the right button becomes active and allows to enter a password manually without picking it from the password list. The length of the password is unlimited.

All the characters are allowed: uppercase, lowercase, numbers, special characters or accents. Moreover, the mix of characters is one of the safety rules in the composition for a password.

This mode is useful when the user does not wish to keep track of this particular password in the future.



Private.ppt Confidential.doc

Please find attached the confidential presentations.

Password: az56£$*hh

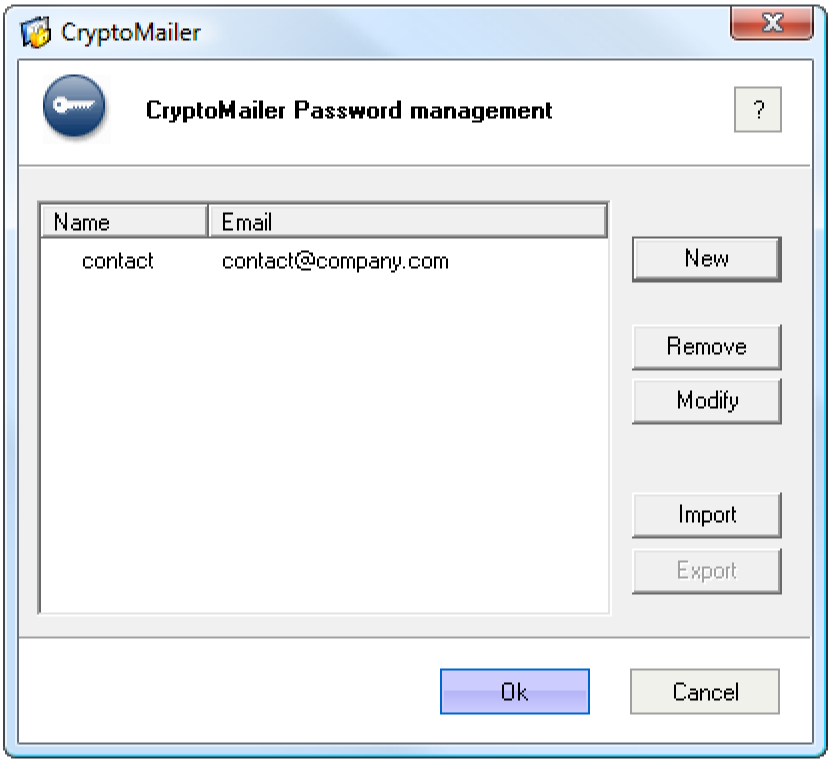
□ Hide password

3. Rules composition of a password
To ensure a good level of safety in protecting access to software or data encryption, it is recommended to follow certain rules of composition of a password.

- Rule1: Use a long password, at least 6 characters, 10 is the perfect length that could ease "brute force" attacks.
- Rule2: Do not be limited to lower case alphabetic characters. Use upper and lower case characters, numbers, special characters (#, &,%,…) or accents (é, ç,...)
- Rule3: Avoiding the use of words or names related to your private life (name of daughter, date of birth, …) or too conventional (password, admin, toto, etc…) that could ease "dictionary" attacks.

4.5 Password Management

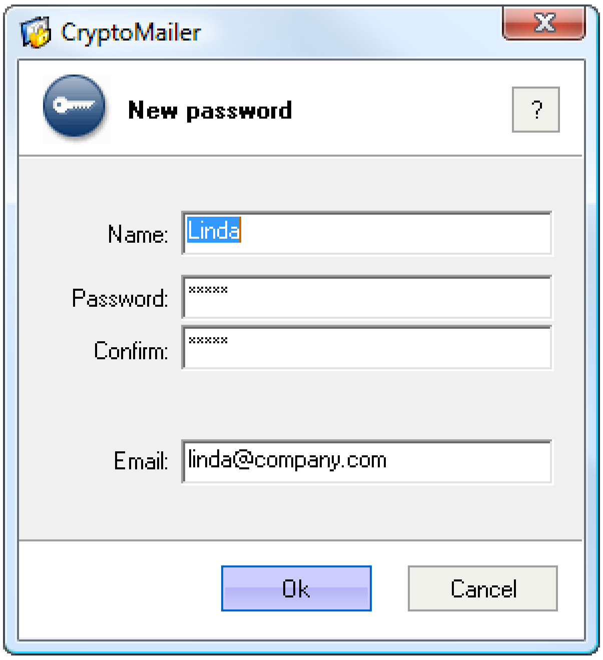
This window is accessible either via "Password" button on the main interface or through the menu "Configuration" > "Password list".
The Password management allows to add, delete, import and export passwords.



Name	Email
contact	contact@company.com

1. Adding a password

Click on the "New" button.


CryptoMailer

New password

Name: Linda

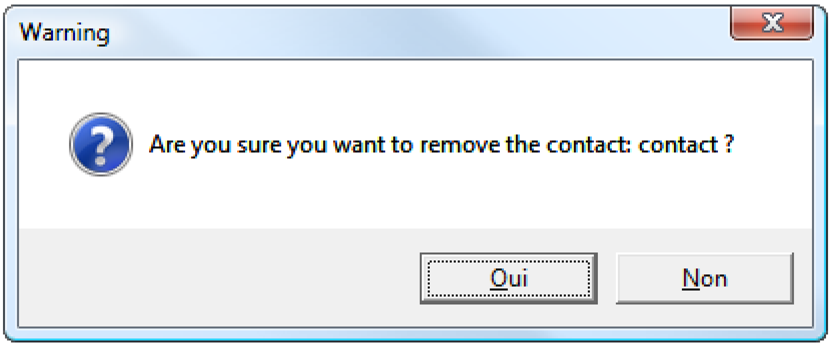
Password: *****

Confirm: *****

Email: linda@company.com

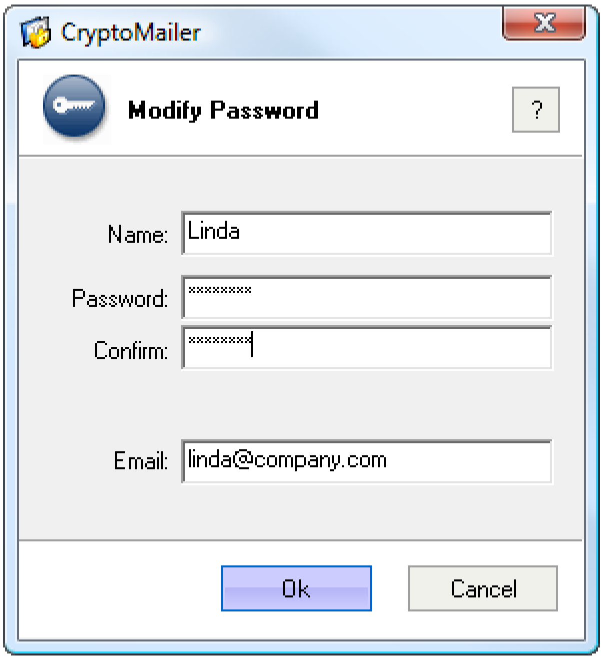
- Enter the "Name" used to represent the password in the list.The password itself will never be displayed. This "Name" is typically the recipient's name.
- Enter the password in the "Password" and then enter it twice in "Confirm" field. See also rules of security in the composition of the password.
- Enter the email address that will be used to send email. This email will be automatically included in the recipient of the encrypted email. This field is optional.
- Click "OK".

2. Delete one or several password
To remove a password, select one or several passwords from the list and click "Delete". To prevent the user to accidentally delete passwords, the next window asks for confirmation.


Warning

Are you sure you want to remove the contact: contact ?

3. Modify password
To change a password, double-click on any password into the list or select it and click "Modify". Each field can be changed individually.



Name: Linda

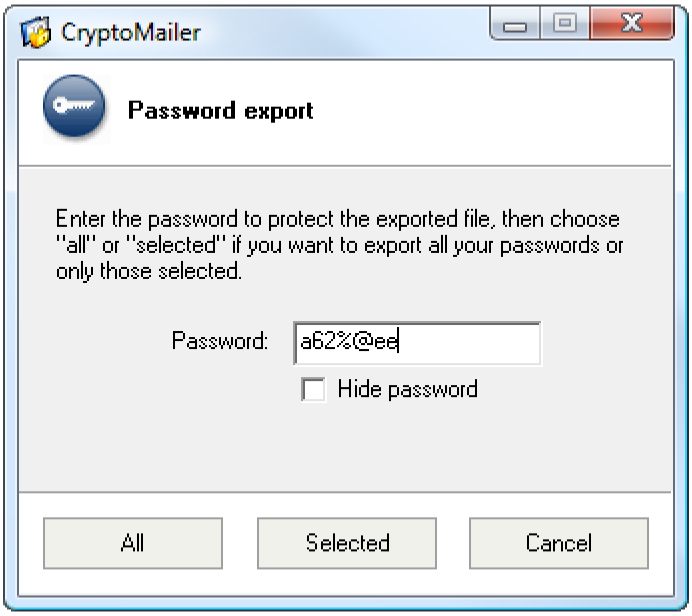
Password: ********

Confirm: ********

Email: linda@company.com

4. Export one or several passwords
CryptoMailer allows you to export all or part of the list of passwords in order to share them more easily. As the export is secured with specific password, communicating a list of password can even be done by email!

To export passwords, select one or several of them from the list, and click on "Export". CryptoMailer asks for your password that will be used to encrypt the file exported. It is possible to export only passwords selected ("Selected") or all passwords ("All").



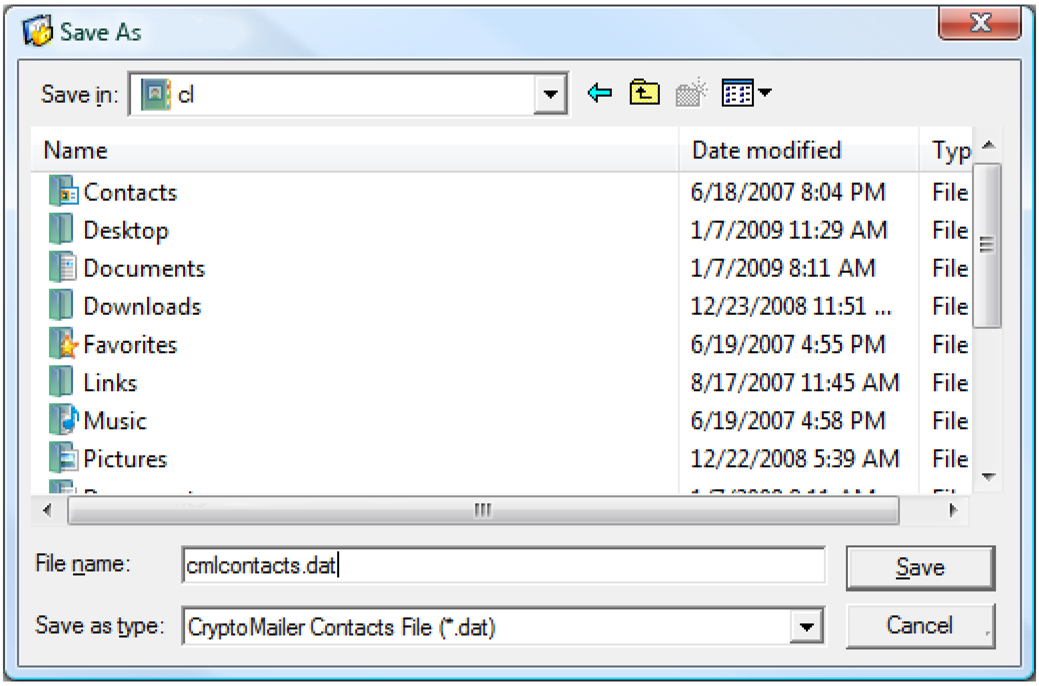
Enter the password to protect the exported file, then choose "all" or "selected" if you want to export all your passwords or only those selected.

Password: a62%@ee

□ Hide password

Se safety rules concerning the composition of the password.

Select directory to save the export file called "cmlcontacts.dat" by default.



Save in: cl

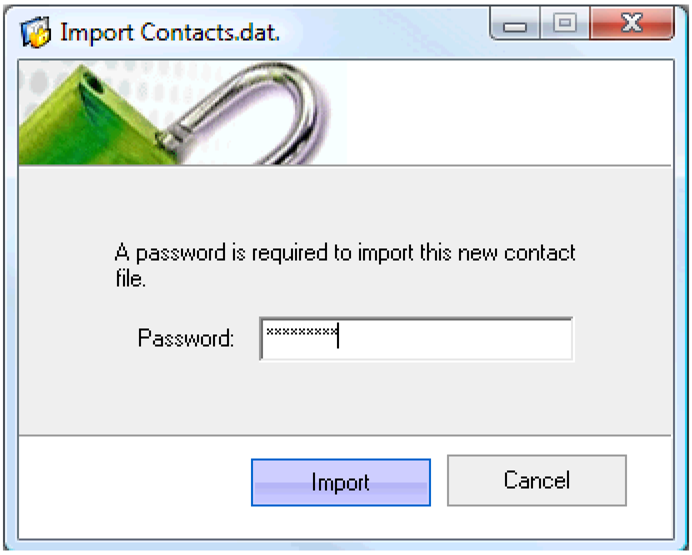
Name	Date modified	Typ
Contacts	6/18/2007 8:04 PM	File
Desktop	1/7/2009 11:29 AM	File
Documents	1/7/2009 8:11 AM	File
Downloads	12/23/2008 11:51 ...	File
Favorites	6/19/2007 4:55 PM	File
Links	8/17/2007 11:45 AM	File
Music	6/19/2007 4:58 PM	File
Pictures	12/22/2008 5:39 AM	File

File name: cmlcontacts.dat

Save as type: CryptoMailer Contacts File (*.dat)

5.Import one or several passwords
CryptoMailer can import passwords. These passwords had to be exported by CryptoMailer software.

To import passwords, click on "Import" button, select the file containing the passwords. CryptoMailer then asks the password used to encrypt the file.



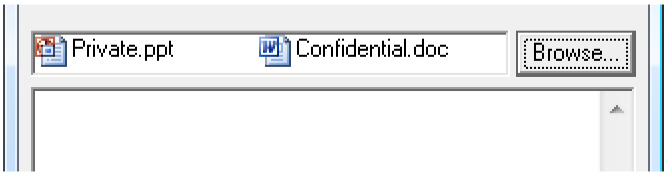
A password is required to import this new contact file.

Password: *********

Passwords contained in the file are then added to the list of the passwords.

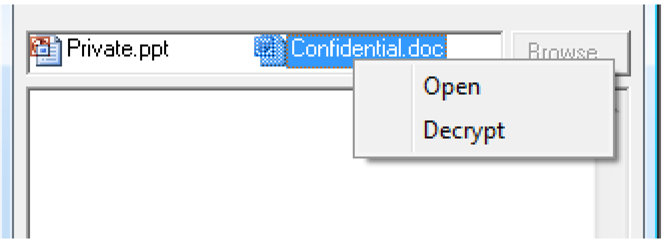
4.6 List of attachments

The list of attachments area shows all the files you have added to be encrypted as shown below.

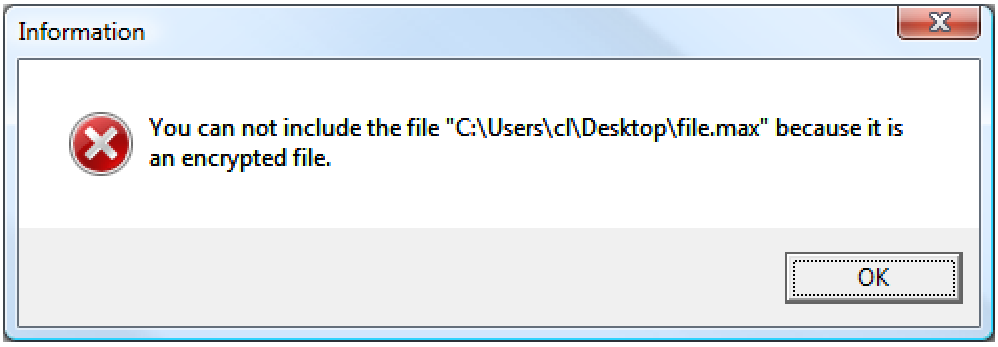


1. **Add one or several files to the list**
    - using a simple drag & drop of your file onto the window (anywhere!),
    - using the "Browse" button.

2. **Contextual menu with right-click on any files**
    - allows to "Remove" the file from the list (when sending encrypted files)
    - allows to "View" or "Decrypt" the file (when receiving encrypted file as shown below)



<u>Note:</u> CryptoMailer does not allow to add a file into an encrypted file (i.e. received via email). If so, the following warning window will popup.:

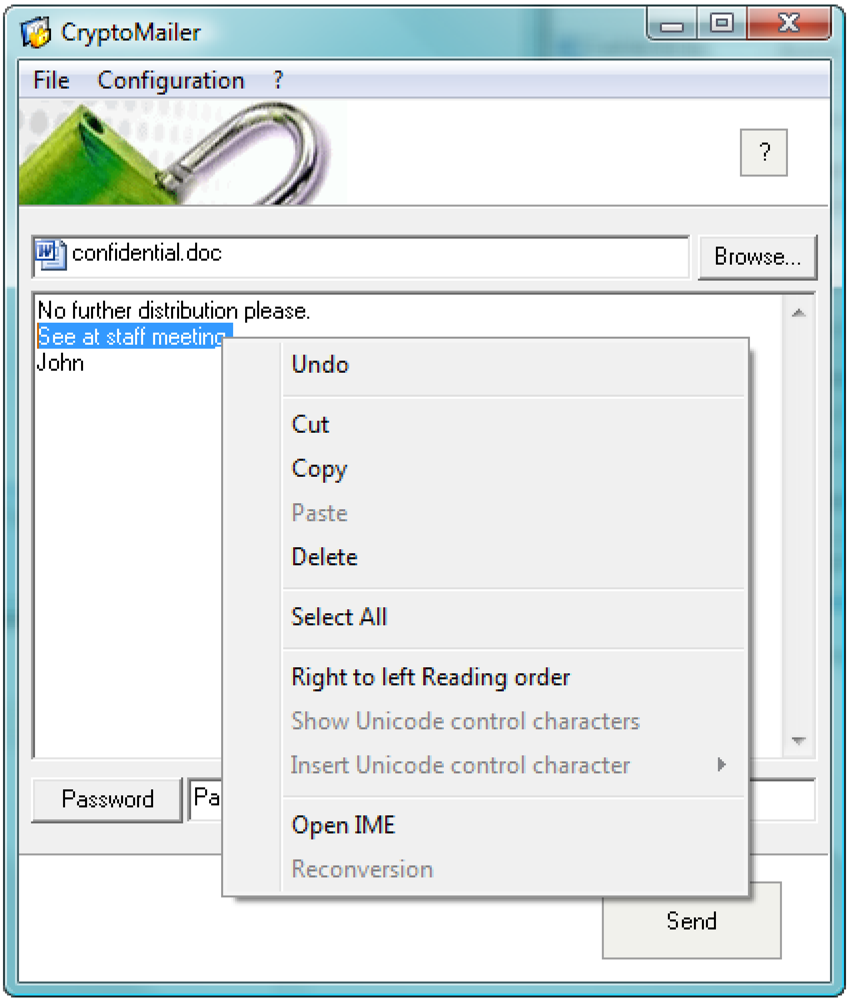

Information

You can not include the file "C:\Users\cl\Desktop\file.max" because it is an encrypted file.

4.7 Adding a text message

The text area can be used to enter a message (memo) in addition to the filesyou want to encrypt. This text message will be encrypted together with the files before sending by email.

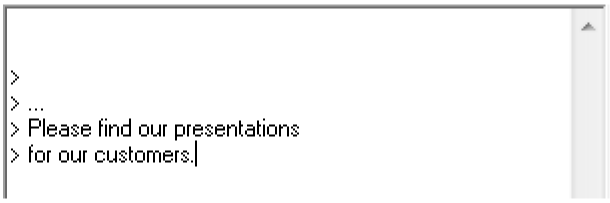
All cut / copy / paste operations are allowed in the text area.



confidential.doc

No further distribution please.
See at staff meeting
John

When the "Answer" button is activated (after receiving an encrypted email), the text area reproduces the text of the sender with the '>' sign and indicates the names of the files received.

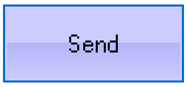


```
>
> ...
> Please find our presentations
> for our customers.
```

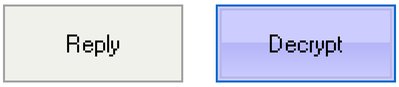
4.8 Encrypt, Decrypt, Send, View

Depending on the context, CryptoMailer proposes several actions via several buttons.

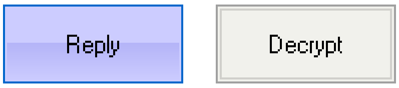
- **When sending an email:**



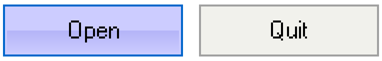
- **Decrypt file when receiving an email:**



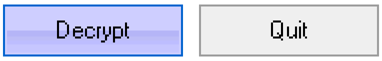
- **When replying to an encrypted email:**



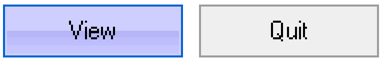
- **When opening an encrypted file:**



- **When decrypting an encrypted file:**



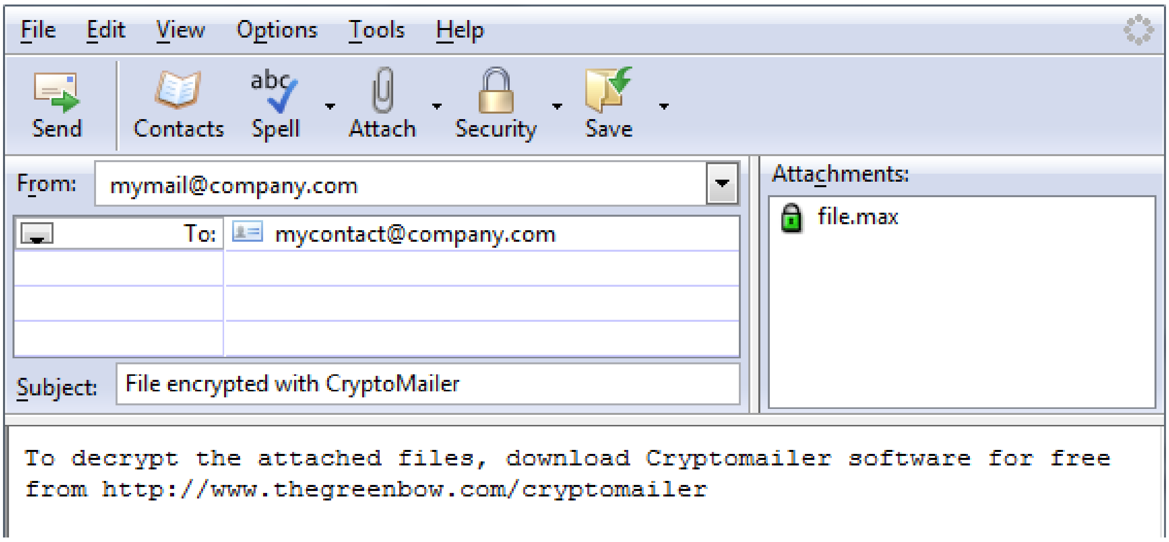
- **When viewing an encrypted file:**



1. Send an encrypted email

By clicking "Send" the default messaging software open an email window, all files from the list and text are grouped into a single encrypted file and attached to that email. The email is fully formatted, ready to be sent.

The email is set with the recipient email address, his name (if configured in the list of passwords), email subject as "encrypted file", a signature in the email body and the encrypted file attached as shown below ("file.max").



From: mymail@company.com

To: mycontact@company.com

Subject: File encrypted with CryptoMailer

Attachments: file.max

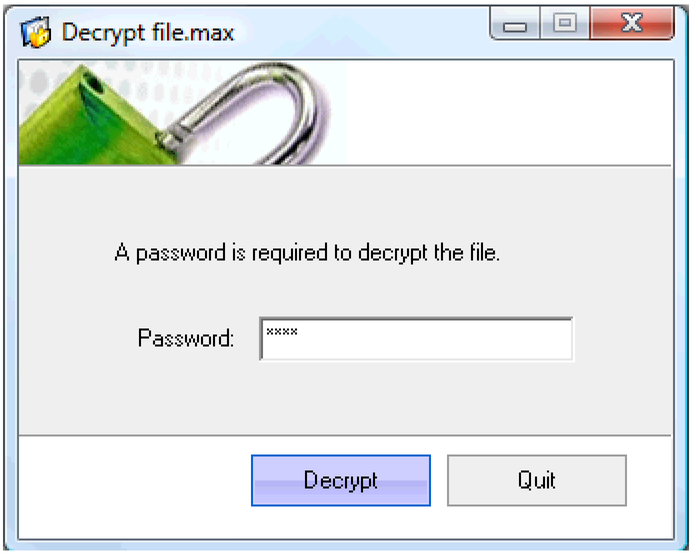
```
To decrypt the attached files, download Cryptomailer software for free
from http://www.thegreenbow.com/cryptomailer
```

The signature in the email body can be changed at any time. To change it, you need to modify "mail.txt", available in the CryptoMailer install directory.

Note: The messaging software that CryptoMailer starts is the one defined by default in Windows. To see which one is set as default, go to 'Control Panel' > 'Internet Options' > 'Programs' tab then "Internet Programs" > "Settings".

2. Decrypt an encrypted file

The user can decrypt an encrypted message located on a drive. The "Decrypt" button allows to select the directory where to decrypt the file in.



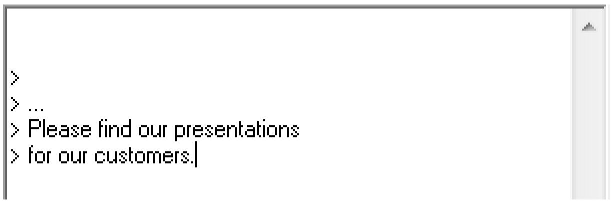
A password is required to decrypt the file.

Password: ****

Note: When decrypting a file, text message in the text area will be saved into a file called 'file.txt' in the same directory.

3. Reply to an encrypted email

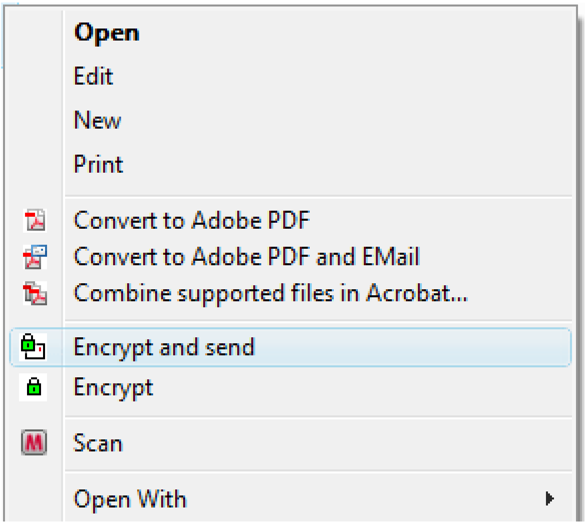
When the "Answer" button is activated (after receiving an encrypted email), the text area reproduces the text of the sender with the '>' sign and indicates the names of the files received.



```
>
> ...
> Please find our presentations
> for our customers.
```

4. Encrypt a file on the disk

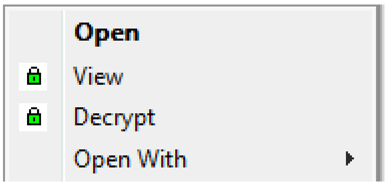
It is possible to encrypt a file on the disk via a right click on the document and then click on 'Encrypt'.



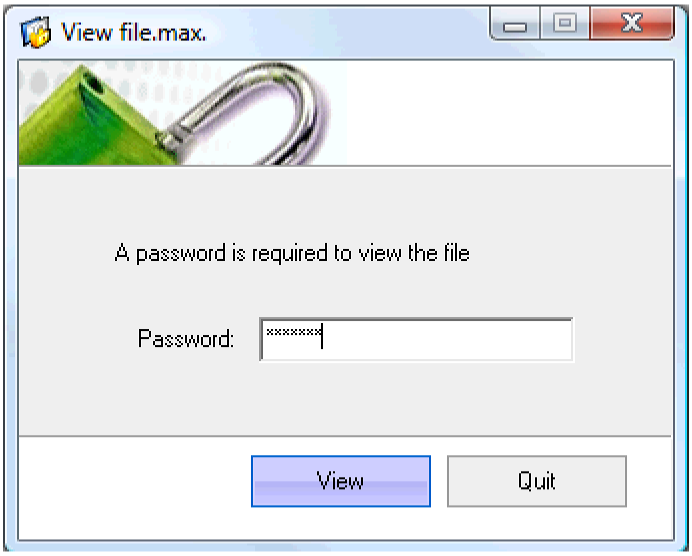
Note: CryptoMailer do encrypt directories.

5. Viewing to an encrypted email

It is possible to view encrypted file via right click on it and click on 'View'.



Software will ask password to decrypt this file or it will find automatically in the contact list if exists already.

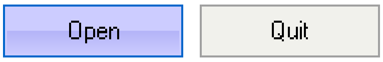


A password is required to view the file

Password: ********

6. Opening CryptoMailer to see which document and text have been received

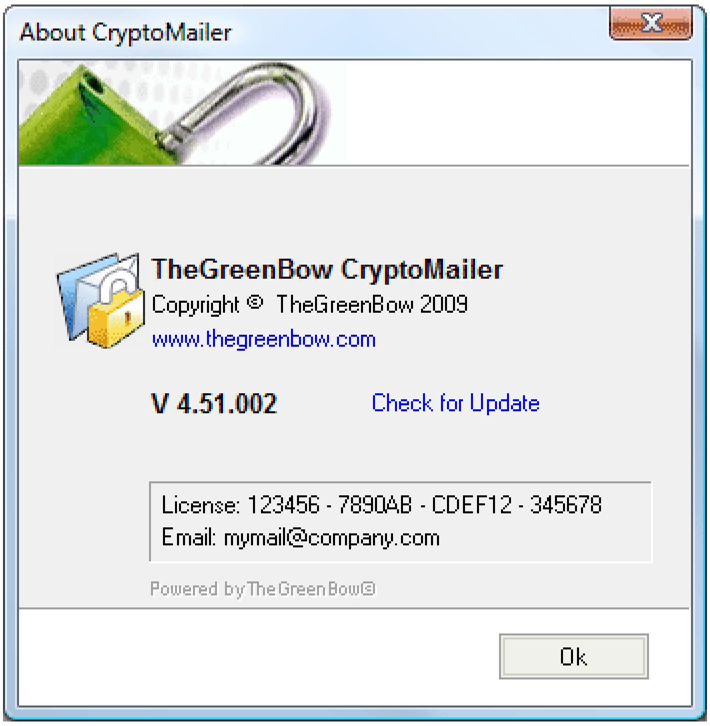
It is possible to open CryptoMailer with an encrypted file to see what text and document it contains via double click on the encrypted file and click on 'Open'.



4.9 About

The "About" menu is accessible through the "?" menu the main interface. It provides information about the software:

- The software release number
- The license number and email when software is activated
- "Check for Update" can check on the TheGreenBow website the availability of an software update.


About CryptoMailer

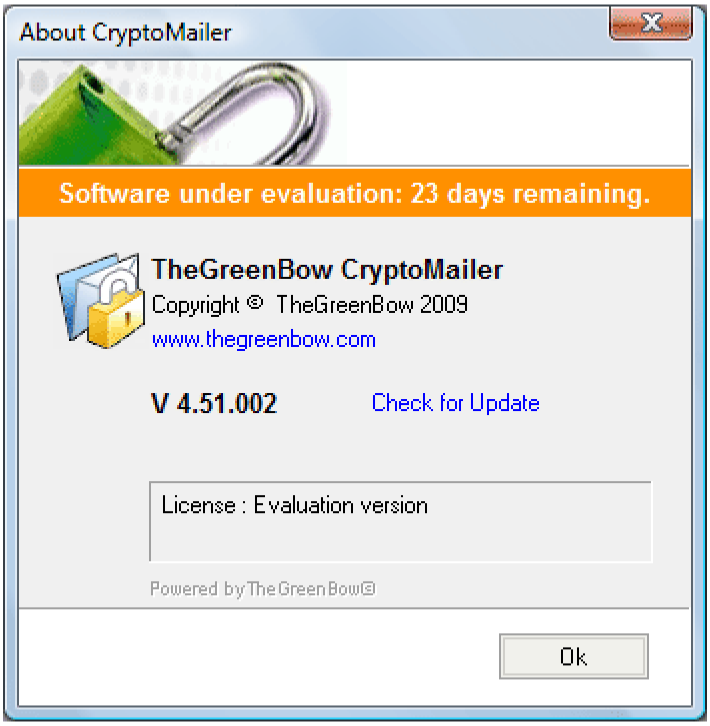
TheGreenBow CryptoMailer
Copyright © TheGreenBow 2009
www.thegreenbow.com

V 4.51.002

License: 123456 - 7890AB - CDEF12 - 345678
Email: mymail@company.com

Powered by TheGreenBow©

If the software is in evaluation period, an orange banner shows the number of days remaining.



About CryptoMailer

Software under evaluation: 23 days remaining.

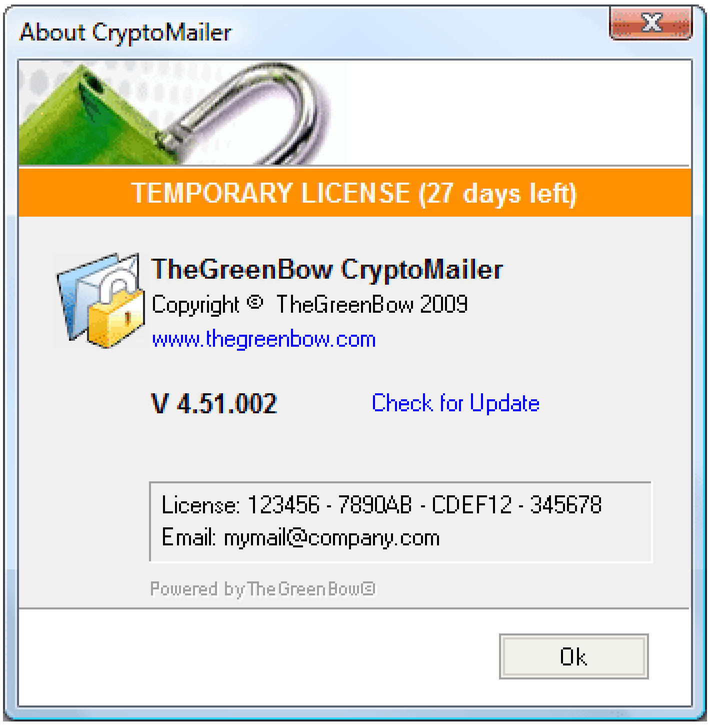
TheGreenBow CryptoMailer
Copyright © TheGreenBow 2009
www.thegreenbow.com

V 4.51.002

License : Evaluation version

Powered by TheGreenBow©

If the software uses a temporary license number, an orange banner shows the number of days remaining.



About CryptoMailer

TEMPORARY LICENSE (27 days left)

TheGreenBow CryptoMailer
Copyright © TheGreenBow 2009
www.thegreenbow.com

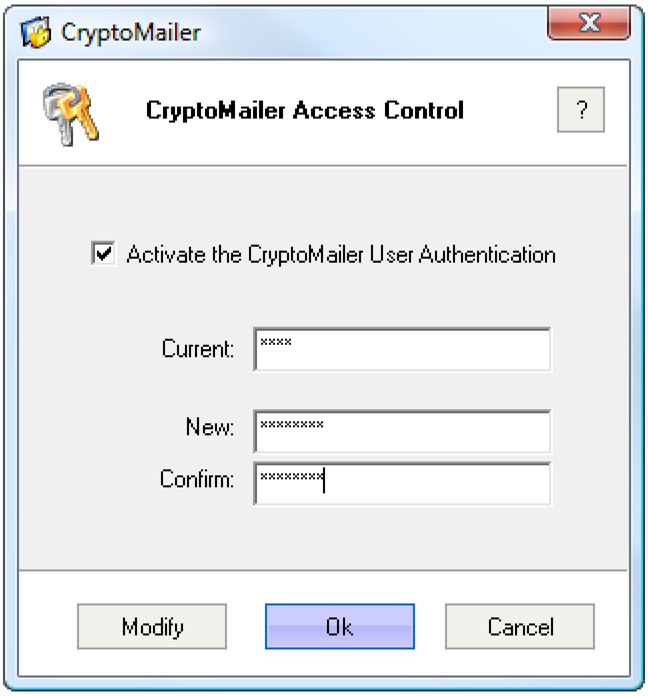
V 4.51.002

License: 123456 - 7890AB - CDEF12 - 345678
Email: mymail@company.com

Powered by TheGreenBow©

4.10 Access control

Access to CryptoMailer can be restricted by a password. To enable password protection, select the "Configuration" > "Access Control". See also rules of security in the composition of the password.



CryptoMailer

CryptoMailer Access Control

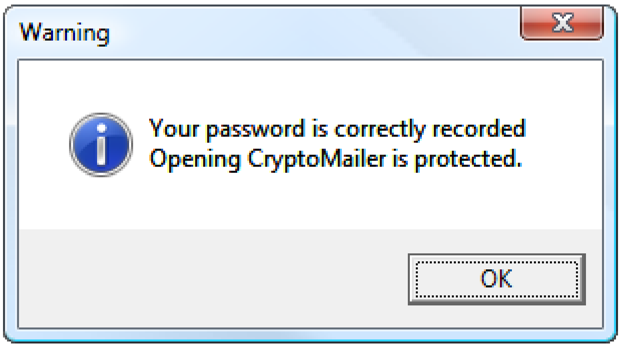
☑ Activate the CryptoMailer User Authentication

Current: ****

New: *********

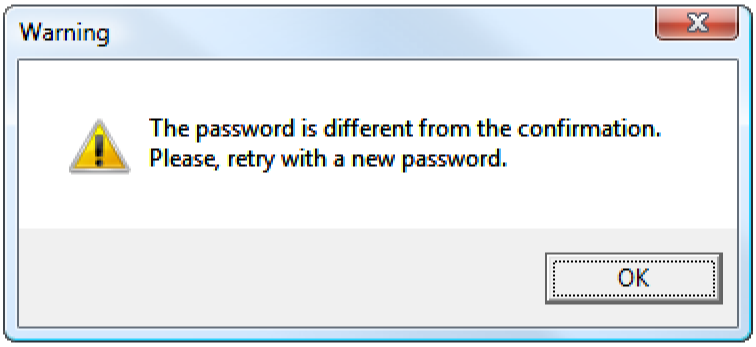
Confirm: *********

Enter your password and click "Ok". In case the password has been set already click "Modify". A confirmation or warning window pops up.



Warning

Your password is correctly recorded
Opening CryptoMailer is protected.



Warning

The password is different from the confirmation.
Please, retry with a new password.

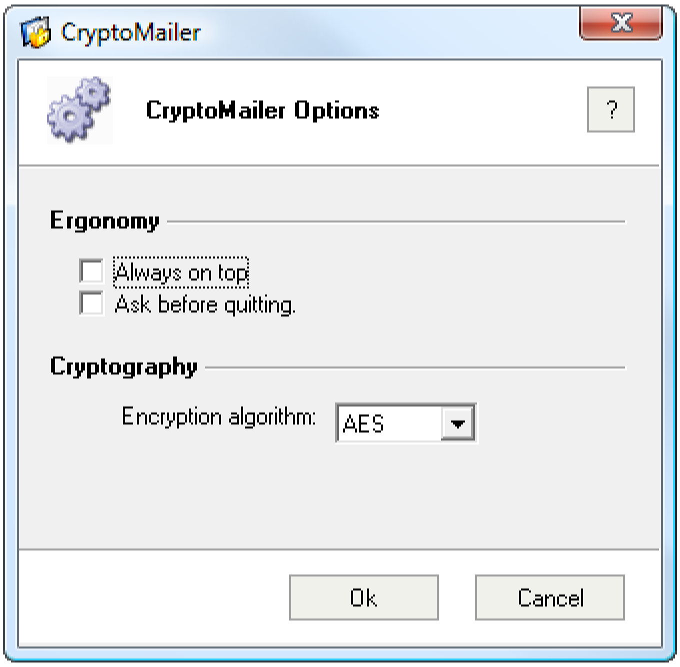
Warning: There is no way to retrieve lost password.

4.11 Options

CryptoMailer options are the following:

- Always on top
- Ask before quiting
- Encryption algorithm: AES or 3DES

To access "Options", go to "Configuration" > "Options".



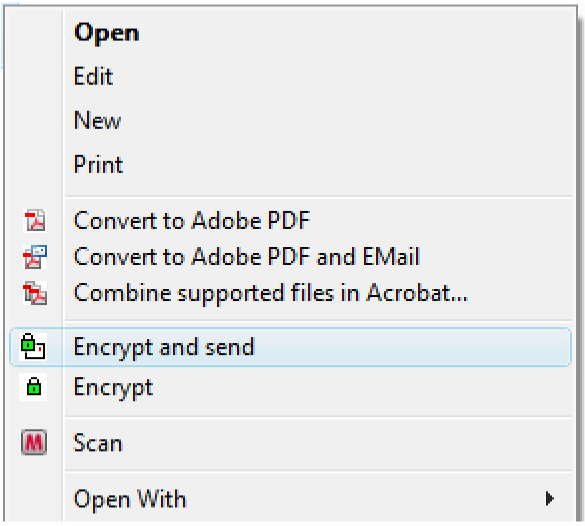
4.12 Drag & Drop

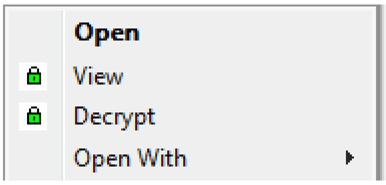
To encrypt a file, simply drag & drop a file from Windows Explorer anywhere onto the CryptoMailer window. The file will be added to the list of attachment.

4.13 Contextual menu

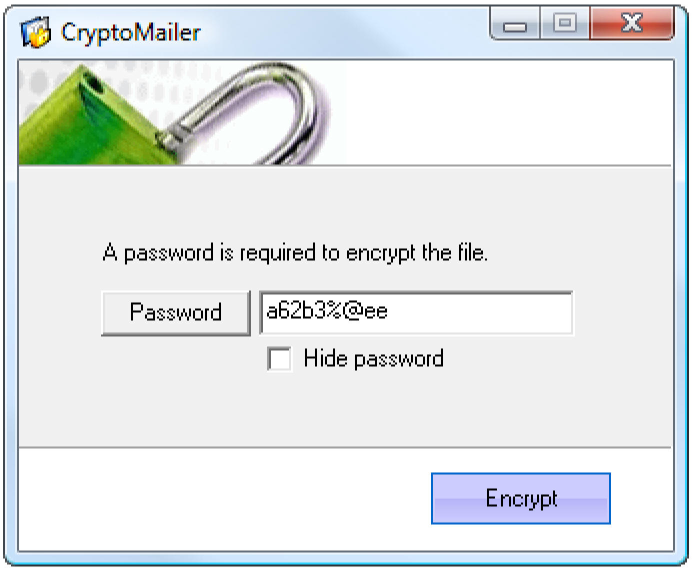
One or several files can be encrypted and sent by email via a right-click as shown below.

- "Encrypt" will encrypt the files in the same directory.
- "Encrypt and Send" will open CryptoMailer with the files in the file area.
- "Decrypt" will decrypt the files in the same directory.
- "View" will open the document assuming the required password is already known in your password list. If not a popup will ask for the password.





To encrypt, a password need to be selected:



A password is required to encrypt the file.

Password: a62b3%@ee

□ Hide password

4.14 Receiving an encrypted file by email

When a message is received in the email software, opening the attachment automatically starts CryptoMailer with the text and list of files in the encrypted file.

If the password used to encrypt the file is part of the list of passwords, CryptoMailer immediately decrypts the file without asking the password to the user.

4.15 Opening an encrypted file

A file encrypted locally (on the hard disk) can be opened:

- By double-clicking the file: CryptoMailer will open its decryption interface
- By right-clicking on the file and selecting the menu "Decrypt": CryptoMailer will decrypt the

file on the disk

If the password used to encrypt the file is part of the list of passwords, CryptoMailer immediately decrypts the file without asking the password to the user.

Part V

Un-installation

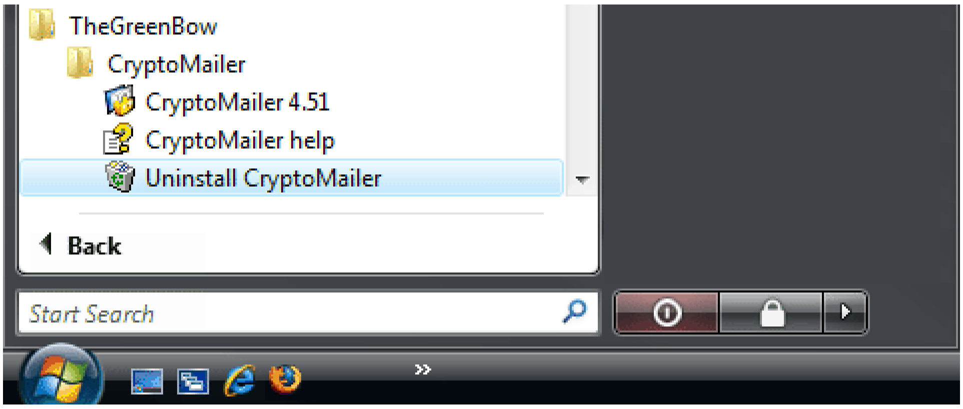
5 Un-installation

5.1 Un-installation

Uninstalling CryptoMailer can be done via the Windows "Start" menu or via the Windows Control Panel:

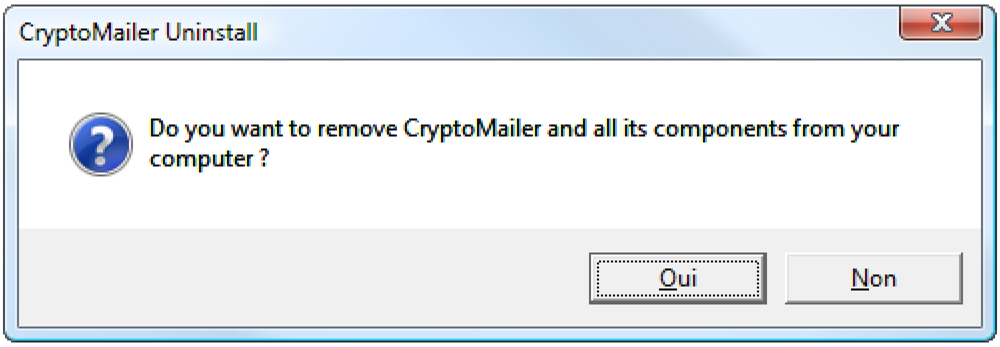
1. Windows "Start" menu

- Select Programs > TheGreenBow > CryptoMailer then "CryptoMailer uninstallation"



2. Windows Control Panel

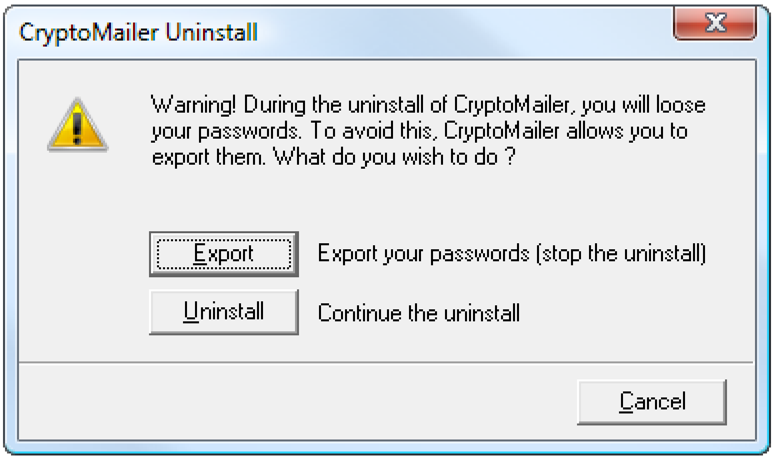
- Select Add/Remove Programs
- Select "CryptoMailer [...]" and click Add/Remove...
- Validate uninstallation windows.


CryptoMailer Uninstall

Do you want to remove CryptoMailer and all its components from your computer ?

Uninstalling warns the user that he risks losing all its keys. It may then as shown below:

- Stop the uninstallation and export its passwords
- Continue uninstalling without saving the passwords
- Cancel uninstallation



CryptoMailer Uninstall

Warning! During the uninstall of CryptoMailer, you will loose your passwords. To avoid this, CryptoMailer allows you to export them. What do you wish to do ?

Export your passwords (stop the uninstall)

Continue the uninstall

Part VI

Contacts

6 Contacts

6.1 Contacts

Information and update are available at: www.thegreenbow.com
Technical support by email at: support@thegreenbow.com
Sales support by email at: sales@thegreenbow.com

Secure, Strong, Simple.

TheGreenBow Security Software